Staff Confidentiality & Security

PURPOSE
To establish standards for the conduct of INSPECT staff as it relates to protecting confidential patient information and storing and retaining sensitive documents and media.

SCOPE
This policy applies to staff of the Indiana Scheduled Electronic Collection and Tracking (INSPECT) Program.

STATEMENT OF POLICY
Given the sensitive nature of daily operational activities at INSPECT, all INSPECT staff are expected to meet strict confidentiality and security standards, including applicable Indiana laws and Federal HIPAA Standards. The staff must not share or discuss details of any INSPECT - specific activities, whether of a technical or non-technical nature, with persons not currently employed by INSPECT or the Professional Licensing Agency. This includes, but is not limited to, sharing or discussing details pertaining to patient medical treatment histories; sharing or discussing details related to INSPECT software functionalities; or sharing or discussing sensitive internal procedural matters. A violation of the confidentiality and security policy will result in disciplinary action commensurate with the offense.

REFERENCES

PROCEDURES
1. *Requesting Patient/Practitioner Information*: INSPECT Staff may submit requests on the PMP Manager/WebCenter to review information referenced by a user, or to evaluate/test the technical performance of the PMP Manager/WebCenter. Any other type of request constitutes a violation of the security and confidentiality policy unless approved by CSAC.

2. *Media Storage/Retention/Disposition*: INSPECT will follow the General Records Retention and Disposition Schedule established by the Commission on Public Records for the Indiana State Records Center unless they are superseded by any Indiana Professional Licensing Agency policies or procedures on record retention.